Attorney's Docket No. 1033048-000019

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Paul Kennedy	Group Art Unit: 2131
Application No.: 09/841,008	Examiner: CHRISTIAN A LAFORGIA
Filed: April 25, 2001	Appeal No.: _____
For: ACCESS AUTHENTICATION FOR DISTRIBUTED NETWORKS	

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated October 7, 2005, finally rejecting claims 9-25, which are reproduced as the Claims Appendix of this brief.

☐ A check covering the ☐ 250 ☐ 500 Government fee is filed herewith.

☒ Charge ☒ $250 ☐ 500 to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

06/08/2006 SZEWDIE1 00000075 09841008

.01 FC:2402 250.00 OP
~~.02 FC:2251 60.00 OP~~

Table of Contents

I. Real Party in Interest

The subject application is assigned to Opsware, Inc., the successor in interest to LoudCloud, Inc.

II. Related Appeals and Interferences

There are no other prior or pending appeals, interferences, or judicial proceedings which may be related to, directly affect or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. Status of Claims

The application contains claims 1-25. Claims 1-8 have been canceled. Claims 9-25 are pending and stand finally rejected, and form the basis for this appeal.

IV. Status of Amendments

There were no amendments filed subsequent to the final Office Action.

V. Summary of Claimed Subject Matter

The claims are directed to the authentication of users to network resources, such as servers, particularly where those resources might be distributed over a variety of locations, such as data centers. Figure 1 of the application illustrates an example of an environment in which the claimed subject matter might be employed. In this example, a number of data centers 108, 110 and 112 in different geographic locations house resource servers 126a-c, 128a-c and 130a-c. A master data center 104 communicates with each of these other data centers. (Page 6, line 22 to page 7, line 8).

As noted in the Background portion of the application, in the past it was conventional to use databases to store authentication information. The use of databases to implement authentication has certain limitations associated with it,

particularly in a distributed environment such as the example illustrated in Figure 1. (Page 2, line 17 to page 4, line 9).

To overcome these limitations, the present application discloses a different approach to store and disseminate the authentication information. More particularly, a directory structure is employed as the mechanism for storing the authentication information. One of the significant advantages of using a directory structure is the fact that it can be easily replicated to a variety of locations, in a much simpler manner than databases.

Figure 2 illustrates an example of a directory structure that implements the features recited in the claims. The directory structure is a hierarchical structure, having a master node 202 at the highest level of the hierarchy. Immediately below the level 202 is a customer level, which contains multiple customer nodes, or accounts 202, 206, 208. Each of these customer accounts forms a subdirectory that relates exclusively to the customer identified in the customer level at the respective nodes 204, 206 and 208.

The subdirectory associated with node 204 illustrates a representative example. The subdirectory contains multiple nodes that are associated with the customer. A "People" node is the parent of a number of subnodes that respectively represent personnel associated with Customer A that have access within Customer A's subtree 204. Each entry corresponding to an individual person contains attributes which represent access credentials for that person. Each of these people will have access rights to only that portion of the resources represented within customer A's account directory subtree 204. In the illustrated example, the nodes within that subdirectory include resources relating to maintenance and financial services, financial and historical records, or individual servers.

An authorized user who appears under the "People" subnode of a particular customer's subdirectory only has access to the resources represented within that subdirectory. Thus, authorized users for Customers B and C do not have access to any of the information contained in the directory subtree 204 associated with Customer A. In the illustrated example, "Paul" is represented in the subdirectories for both Customer A and Customer C. Thus, he has access to the resources of each of those two customers. (Page 11, line 18 to page 13, line 3).

Referring again to Figure 1, a master directory structure 102, such as that illustrated in Figure 2, is maintained by a directory server within the master data center 104. This master data center also contains a duplicate 106 of the master directory which is used to replicate the directory structure at the remote data centers 108, 110 and 112. In the illustrated example, multiple copies of the replicated directory structure are stored in each data center. For instance, the remote data center 108 houses two copies 114, 116 of the directory structure. Each replicated copy of the directory structure has an associated directory server to provide information from the stored directory to the individual devices, e.g. servers 126-130, within the respective data centers. (Page 8, lines 7-27).

By means of this arrangement, the master directory structure 102 is not directly accessed by the resources within the remote data centers 108, 110, 112. Since each data center contains its own copy of the directory structure, delays or denial of service that might be caused by data traffic congestion or failure of communication links is avoided. Furthermore, security is enhanced by requiring a resource to only contact a directory server within its respective data center. (Page 9, lines 8-23).

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents two grounds of rejection for review on this appeal:

1. Claims 9-12, 14-18, 20-23 and 25 stand rejected under 35 U.S.C. §103, as being unpatentable over the Aldred et al patent (US 6,438,549) in view of the Byrne et al patent (US 6,708,170); and

2. Claim 13, 19 and 24 stand rejected under 35 U.S.C. §103 as being unpatentable over the Aldred and Byrne patents, in further view of the Pang patent (US 6,446,204).

VII. Argument

A. Claims 9, 16 and 21

Independent claim 9 recites a method for authenticating users to individual network devices that are distributed among a plurality of locations. Independent claim 16 recites a data center comprising a plurality of network resources and a directory server. Independent claim 21 recites a distributed network having network resources distributed among a plurality of locations. Among other elements, each of these three claims recites a directory structure that is stored at a location within the network, and specifically in the case of claim 16, at a data center. The claims recite that the directory structure comprises a root node, a first level of nodes below the root node that are associated with respective organizations to which network resources are assigned, and at least one further level of nodes below the first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first level node, and authentication information for those users.

Each of claims 9, 16 and 21 stands finally rejected as being obvious over the Aldred patent in view of the Byrne patent. MPEP § 2143 sets forth three criteria that must be met to establish a prima facie case of obviousness. One of these criteria is that "the prior art reference (or references when combined) must teach or suggest all the claim limitations." The rejection of claims 9, 16 and 21 fails to meet at least this requirement.

In rejecting the claims, the final Office Action asserts that the above-noted subject matter recited in each of claims 9, 16 and 21 is disclosed in the Aldred patent, with specific reference to Figures 1, 2 and 7, as well as column 3, line 64 to column 4, line 20, and column 6, lines 51-60. In the cited passage at columns 3 and 4, the Aldred patent discloses the general structure of a directory tree. It does not, however, disclose a directory having the particular features recited in the claims, namely a root node, a first level of nodes below the root node associated with respective organizations, and at least one further level of nodes that identify users who are authorized to access the network devices.

Nor does it suggest the use of a directory structure as the mechanism to store information for authenticating users to network resources. Insofar as access control

is concerned, the Aldred patent discloses the use of access control lists (ACLs), beginning at column 4, line 65. Referring to the disclosure beginning at column 5, line 17, as well as Figure 5, the Aldred patent discloses that the ACL information is stored in a relational database management system 39. The passage at column 6, lines 51-60, cited in the Office Action, relates to one of the tables that are stored in the relational database.

Thus, unlike the claimed subject matter, the Aldred patent does not disclose that access control information is contained at certain nodes within the directory tree itself. Rather, the patent is representative of the prior art described in the background portion of the present application, in which access control information is stored in a database. As can be seen in Figure 5, the database 39 is distinct from the directory server 37.

Since the Aldred patent does not disclose a directory structure that is arranged in the manner recited in claims 9, 16 and 21 to store access information, it also does not disclose other features recited in the claims. For example, claim 9 recites a step which is responsive to a request by a user for access to one of the network devices to determine the organization to which that device is assigned and "whether said user is identified on a node below the first-level node associated with the determined organization." In the system of the Aldred patent, access control is determined with reference to the permissions table 47 stored in the relational database. It does not determine whether a user is identified on a node at a particular level of the directory tree.

The Byrne patent was cited for its disclosure of replicating authentication information at individual servers. However, it does not overcome the above-noted differences between the claimed subject matter and the disclosure of the Aldred patent. In particular, it does not disclose the use of a directory structure to maintain authentication information associated with different organizations, in the manner recited in claims 9, 16 and 21.

Accordingly, the Aldred and Byrne patents, whether considered individually or in combination, do not teach or suggest all of the subject matter recited in the claims. For at least this reason, a prima facie case of obviousness has not been established.

B. Claims 10, 17 and 22

Claim 10 recites that the directory includes nodes below the first level that identify resources of an organization to which authenticated users are allowed access. Claims 17 and 22 recite similar subject matter.

The final Office Action asserts that this claimed subject matter is disclosed in the Aldred patent, at column 4, line 65 to column 5, line 16. However, this portion of the patent does not pertain to the information stored at certain levels of a directory. Rather, as noted previously, it deals with the Access Control Lists, which are separate from the LDAP directory. There is no teaching in the Aldred patent regarding the type of information stored of various levels within a directory. In particular, there is no teaching of storing resources in relation to an organization to which users are allowed access, as recited in the claims.

C. Claims 14, 18 and 23

These claims recite that the same user identification and authentication information is contained at a plurality of nodes respectively associated with different first-level nodes. In rejecting these claims, the final Office Action again refers to the Aldred patent at column 14, line 65 to column 5, line 16. For the reasons presented above, this portion of the patent does not support the rejection. It has nothing to do with the type of information stored in particular nodes of the directory, let alone teach that the same information is stored in plural nodes.

D. Claims 13, 19 and 24

Claim 13 depends from claim 9, and recites that at least some of locations contain at least two replicated copies of the directory structure. The claim recites the further step of distributing access requests among the replicated copies by means of a load balancer. Claims 19 and 24 also recite the concepts of having at least two directory servers and a load balancer that distributes requests for access to resources among the directory servers.

In the rejection of claims 13, 19 and 24, the Pang patent was cited as disclosing at least two replicated copies of a directory structure, and distributing access requests among the replicated copies by means of a load balancer. While

the cited passage at column 23, lines 50-64, discloses the use of a load balancing scheme to balance the workload of multiple authentication hosts, it does not disclose the use of a directory structure to store the identification of users who are authorized to access network resources, as discussed above. Hence, the Pang patent also does not overcome the distinctions between the claimed subject matter and the disclosure of the Aldred patent.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

(none)

X. Related Proceedings Appendix

(none)

Respectfully submitted,

Buchanan Ingersoll PC

Date June 7, 2006

By: 

James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703.836.6620

VIII. CLAIMS APPENDIX

The Appealed Claims

9. A method for authenticating users to individual network devices that are distributed among a plurality of locations, comprising the following steps:

storing a directory structure at one of said locations, said directory structure comprising a root node, a first level of nodes below said root node that are associated with respective organizations to which said network devices are assigned, and at least one further level of nodes below said first level that identify users who are authorized to access the network devices assigned to the organization associated with a parent first-level node and authentication information for said users;

replicating said directory structure among said plurality of locations;

in response to a request by a user for access to one of said network devices, determining which organization to which said one device is assigned and whether said user is identified on a node below the first-level node associated with the determined organization; and

authenticating said user to said device if the user is so identified.

10. The method of claim 9, wherein said directory structure further includes nodes below said first level that identify resources of an associated organization to which authenticated users are allowed access.

11. The method of claim 9, wherein said determining step is performed with reference to a replicated copy of said directory structure at the location containing said one device.

12. The method of claim 9 wherein said network devices comprise servers, and said locations are data centers.

13. The method of claim 9, wherein at least some of said locations contain at least two replicated copies of said directory structure, and further including the steps of distributing access requests among said replicated copies by means of a load balancer.

14. The method of claim 9, wherein the same user identification and authentication information is contained at a plurality of said further level nodes that are respectively associated with different ones of said first-level nodes.

15. The method of claim 9, wherein said replicating step is carried out automatically without user input.

16. A data center comprising a plurality of network resources and a directory server for authenticating users for access to said network resources by means of a directory structure comprising a root node, a first level of nodes below said root node that are associated with respective organizations to which said network resources are assigned, and at least one further level of nodes below said first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first-level node and authentication information for said users.

17. The data center of claim 16, wherein said directory structure further includes nodes below said first level that identify resources of an associated organization to which authenticated users are allowed access.

18. The data center of claim 16, wherein the same user identification and authentication information is contained at a plurality of said further level nodes that are respectively associated with different ones of said first-level nodes.

19. The data center of claim 16, comprising at least two of said directory servers, and further including a load balancer that distributes requests for access to said resources among said directory servers.

20. The data center of claim 16, wherein at least some of network resources are servers that each include an authentication module that is responsive to a request for access to determine the organization to which its corresponding server is assigned and restrict directory searches to the further-level nodes below the first-level node associated with the determined organization.

21. A distributed network having network resources distributed among a plurality of locations, and comprising:

a master directory server at one of said locations, said master directory server containing a directory structure comprising a root node, a first level of nodes below said root node that are associated with respective organizations to which said network resources are assigned, and at least one further level of nodes below said first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first-level node and authentication information for said users; and

at least one directory server at each of the other locations, each of said directory servers containing a replicated copy of said directory structure.

22. The distributed network of claim 21, wherein said directory structure further includes nodes below said first level that identify resources of an associated organization to which authenticated users are allowed access.

23. The distributed network of claim 21, wherein the same user identification and authentication information is contained at a plurality of said further level nodes that are respectively associated with different ones of said first-level nodes.

24. The distributed network of claim 21, wherein at least some of said locations contain at least two directory servers, and further including a load balancer that distributes requests for access to said resources among said directory servers.

25. The distributed network of claim 21, wherein at least some of network resources are servers that each include an authentication module that is responsive to a request for access to determine the organization to which its corresponding server is assigned and restrict directory searches to the further-level nodes below the first-level node associated with the determined organization.